**2.3- SSH con clave pública/privada**

* En el archivo de configuración, descomentamos la línes de AuthorizedKeys e indicamos la ruta donde se va a encontrar el archivo de las claves autorizadas.
* En el CLIENTE, dentro de la carpeta /home/nombredeusuario, creamos la carpeta .ssh
* En esa carpeta generamos las claves mediante ssh-keygen.
* Enviamos la clave pública (acaba en .pub) al servidor.
  + NOTA: Utilizando el siguiente comando, copiamos directamente la clave en el servidor, sin necesidad de realizar los pasos posterioriores: ssh-copy-id -i /clave.pub usuario@direcciónip
* Dentro del servidor, añadimos la clave pública al archivo de claves (cat origen >> destino)
* Es posible que el archivo de claves no esté habilitado (lo habilitamos en /etc/ssh/sshd\_config) así como la posibilidad de autenticarnos mediante clave pública, puede también que el archivo authorized\_keys no esté creado (lo creamos con touch authorized\_keys).
* Para añadir seguridad, en el archivo de configuración, podemos añadir PasswordAuthentication no, de tal manera que solo nos deje autenticarnos mediante clave pública.
* La conexión desde el cliente ya debe autenticarse automáticamente con las claves pública/privada.

**POSIBLES ERRORES:**

-Cuidado al añadir la clave al archivo authorized\_keys, no debemos tocar nada mediante editor de texto ya que puede dar error.

-Cuidado con cómo están conectadas las máquinas virtuales.

-Reinicia el servicio si es necesario.